UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/783,843	02/15/2001	James Alexander Reeds III	1999-0274	2575

7590 09/08/2004

Charles A Mirho
112 W 37th St
Vancouver, WA 98660

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/783,843	REEDS ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 April 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/15/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-28 have been examined.

Specification

2. The disclosure is objected to because of the following informalities: "WE CLAIM:" in the last page of the specification (p. 13, line 21) should be moved to the top of the claim section on page 14.

Appropriate correction is required.

Claim Objections

3. Claims 1, 7, 10, 18, 20 and 22 are objected to because of the following informalities:

a. Regarding claim 1, "an integrity" (9^{th}-10^{th} lines) should be changed to "the integrity".

b. Regarding claims 7, 10, 18 and 20, the term "encrypted payload data" should be changed to "encrypted data packet". According to the specification, a data packet includes a data payload and a checksum value for the data payload; the data packet is then encrypted to produce an encrypted data packet for transmission to the receiver (fig. 3).

c. Regarding claim 22, "at" (6^{th} line) should be changed to "and".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 7 and 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claim 7, it recites the limitation "comparing the encrypted payload data to the network layer checksum to detect the key stream out-of-synchronization" in 5^{th}-6^{th} lines. It is not clear what the limitation means because the encrypted payload data cannot be compared to the network layer checksum. The limitation is interpreted as "decrypting, using a key stream, the encrypted data packet to produce decrypted payload data and a received checksum, calculating a checksum based on the decrypted payload data; and detecting, at the network layer, the key stream loss of synchronization if the calculated checksum is not equal to the received checksum" (see specification, fig. 6).

b. Claim 18 is rejected on the same basis as claim 7. The limitation "to compare the encrypted payload data to the network layer checksum to detect the key stream out-of-synchronization" (the 8^{th}-9^{th} lines) is interpreted as "to decrypt, using a key stream, the encrypted data packet to produce decrypted payload data and a received checksum, to calculate a checksum based on the decrypted payload data; and to detect, at the network layer, the key stream loss of synchronization if the calculated checksum is not equal to the received checksum

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-4, 11-14 and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lockhart et al. (5,841,873) in view of Ahmed et al. (6,747,961).

a. Regarding claim 1, which is representative of clams 11 and 24-28, Lockhart discloses a method comprising:

receiving an encrypted data packet through a wireless communication channel (fig. 1; fig. 2, step 213);

decrypting the encrypted data packet to produce a decrypted data packet (fig. 2, step 215);

calculating a payload checksum based on a payload of the decrypted data packet (fig. 2, steps 223; col. 4, lines 54-66) and

comparing a checksum within the decrypted data packet to the payload checksum to determine the integrity of the payload (fig. 2, step 221).

Lockhart does not disclose calculating the payload checksum at a network layer. However, Examiner takes Official Notice that using Transmission Control Protocol (TCP), which is part of a network layer (specification page 6, lines 22-24), to determine

the integrity of a transmitted payload is well known in the art. In particular, the transmitting TCP calculates a checksum based on the payload data to be transmitted and includes the checksum in the TCP header for transmission; the receiving TCP then performs the same calculation on the payload data received and compares the result with the received checksum; a discrepancy indicates some error. It would have been obvious at the time of the invention was made to one of ordinary skill in the art to calculate the payload checksum at a network layer since Examiner takes Official Notice that using TCP to determine the integrity of a transmitted payload data is well known in the art.

Lockhart does not disclose a security sub-network layer performing decryption. Ahmed discloses a security sub-network layer located below a network layer and above the MAC layer, the security sub-network layer providing encryption/decryption function to a network layer (col. 3, lines 53-59; fig. 3B). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the security sub-network layer of Ahmed into the method of Lockhart, the sub-network layer providing encryption/decryption function to a network layer. Such a sub-network protocol layer provides the communication systems with various mobility management functions (col. 3, lines 59-63).

b. Regarding claims 2 and 12, Lockhart further discloses determining the payload is not valid if the payload checksum does not equal the received network layer header checksum (fig. 2, step 300).

c. Regarding claims 3 and 13, Lockhart further discloses receiving the encrypted data packet at a data link layer (fig. 1, element 109).

Regarding transferring the encrypted data packet to the sub-network security layer from the data link layer, the sub-network security layer of Ahmed in claim 1 located above the MAC layer (col. 3, lines 53-59).

d. Regarding claims 4 and 14, Lockhart further discloses resetting the data link layer if the payload checksum does not equal the received network layer header checksum (fig. 3, step 317).

8. Claims 5-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lockhart in view of Ahmed as applied to claim 1 above, and further in view of Latka (5,646,996).

a. Regarding claim 5, Lockhart further discloses prior to receiving the encrypted data packet, forming the encrypted data packet using the payload and the network layer header checksum (fig. 2, step 209); and transmitting the encrypted data packet through the wireless channel at the data link layer (fig. 2, step 211). Lockhart does not disclose calculating a second checksum based on the payload at the network layer and comparing the second checksum to the network layer header checksum. Latka discloses a method for determining whether a key stream at the transmitting side is out of sequence by calculating a second checksum based on current state of the key stream generator in memory, comparing the second checksum to a first checksum previously generated based on the same data (col. 2, line 30 – col. 3, line 16). It would

have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Lockhart and Ahmed to calculate a second checksum on the transmitting side and compare the second checksum to a previously calculated checksum, both of which calculated based on the same data, as taught by Latka. Accordingly, the data is the payload at the network layer. The motivation for doing so would have been to detect whether a key stream is out of synchronization at the transmitting side due to a temporary loss of power (col. 3, lines 10-13).

b. Regarding claim 6, Lockhart further discloses encrypting the payload and the network layer header checksum (fig. 2, step 209).

9. Claims 7, 10, 18 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lockhart in view of Menezes et al. ("Handbook of Applied Cryptography"). Regarding claims 18 and 21, which are representative of claims 7 and 10, Lockhart discloses a system for detecting key out of out of synchronization comprising:

an encryption engine configured to encrypt a data packet including a checksum to produce an encrypted data packet having an embedded checksum (fig. 2, step 209; col. 4, lines 54-66);

a transmitter configured to transmit the encrypted data packet through a wireless channel to a decryption engine (fig. 2, step 211; fig.1, element 109);

a checksum validation engine comprising

a decryption engine configured to decrypt the encrypted data packet to produce decrypted payload data and a received checksum (fig. 2, step 215);

a checksum generator configured to calculating a checksum based on the decrypted payload data (fig. 2, step 223); and

the checksum validation engine configured to detect the key loss of synchronization if the calculated checksum is not equal to the received checksum (fig. 2, step 221; col. 2, lines 25-31; col. 3, lines 11-15).

Lockhart does not disclose that the checksum in the data packet is calculated at a network layer on the transmitting side and that a second checksum is calculated and compared to a received checksum at a network layer on the receiving side. However, Examiner takes Official Notice that transmitting Transmission Control Protocol (TCP), which is part of a network layer, calculates a checksum based on the payload data to be transmitted and includes the checksum in the TCP header for transmission and that receiving TCP performs the same calculation on the payload data received and compares the result with the received checksum to detect errors is well known in the art. It would have been obvious at the time of the invention was made to one of ordinary skill in the art to calculate the payload checksum by the transmitting TCP and to calculate a second checksum and compare the second checksum to a received checksum by the receiving TCP since Examiner takes Official Notice that calculating the payload checksum by the transmitting TCP and to calculate a second checksum and compare the second checksum to a received checksum by the receiving TCP is well known in the art.

Lockhart does not disclose that the encryption algorithm is a stream cipher. Menezes discloses using stream ciphers (p. 161, see 6.1 Introduction). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lockhart to use a stream cipher, as taught by Menezes, because stream ciphers are advantageous in situations where transmission errors are highly probable.

10. Claims 8-9 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lockhart in view of Menezes as applied to claim 7 above, and further in view of Ahmed.

a. Regarding claims 8 and 19, Lockhart does not disclose a security sub-network layer performing encryption. Ahmed discloses a security sub-network layer providing encryption/decryption function to a network layer (fig. 3B). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the security sub-network layer of Ahmed into the method of Lockhart, the sub-network layer providing encryption/decryption function to a network layer. Such a sub-network protocol layer provides the communication systems with various mobility management functions (col. 3, lines 59-63).

b. Regarding claims 9 and 20, Lockhart further discloses transmitting the encrypted payload data through a wireless channel at a data link layer (fig. 1, element 109).

11. Claims 15-17 and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lockhart in view of Latka.

a. Regarding claim 22, which is representative of claims 15-16, Lockhart discloses an apparatus comprising:

an encryption engine configured to encrypt a payload and the payload checksum to form the encrypted data packet (fig. 2, step 209); and

a transmitter adapted to transmit the encrypted data packet to a receiver (fig. 2, step 211).

Lockhart does not disclose that the payload checksum is a network layer checksum. However, Examiner takes Official Notice that Transmission Control Protocol (TCP), which is part of a network layer (specification page 6, lines 22-24), calculates a checksum based on the payload data to be transmitted and includes the checksum in the TCP header for transmission is well known in the art. It would have been obvious at the time of the invention was made to one of ordinary skill in the art to calculate the payload checksum at a network layer since Examiner takes Official Notice that transmitting TCP calculates a checksum of a payload data to be transmitted and includes the checksum in the TCP header for transmission is well known in the art.

Lockhart does not disclose a checksum generator configured to calculate a transmitter payload checksum based on the payload and a checksum validation engine configured to compare the transmitter payload checksum to the network layer check sum at the network layer. Latka discloses an apparatus for determining whether a key stream at the transmitting side is out of sequence, the apparatus comprising a

checksum generator configured to calculate a second checksum based on the current state of the key stream generator in memory, a checksum validation engine configured to compare the second checksum to a first checksum previously generated based on the same data (col. 2, line 30 – col. 3, line 16). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Lockhart to include a checksum generator configured to calculate a second checksum on the transmitting side and a checksum validation engine configured to compare the second checksum to a previously calculated checksum, both of which calculated based on the same data, as taught by Latka. Accordingly, the data is the payload at the network layer. The motivation for doing so would have been to detect whether a key stream is out of synchronization at the transmitting side due to a temporary loss of power (col. 3, lines 10-13).

b. Regarding claims 17 and 23, Lockhart further discloses that the transmitter is adapted to transmit the encrypted data packet through a wireless communications channel (fig. 1, element 109).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Gutman et al. (5,130,993) discloses transmitting encoded data on unreliable networks.

Chapman et al. (5,926,468) discloses wireless communications systems and methods utilizing data link reset.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
9/7/04

Gilberto Barron

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100